PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-049766
(43)Date of publication of application : 18.02.2000

(51)Int.Cl. H04L 9/08
H04L 9/32

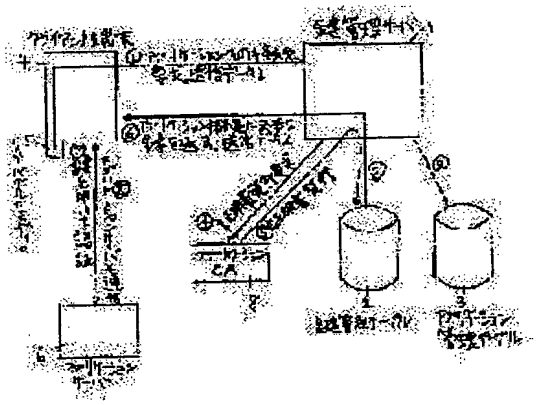
(21)Application number : 10-210672
(22)Date of filing : 27.07.1998

(71)Applicant : HITACHI LTD
HITACHI SOFTWARE ENG CO LTD

(72)Inventor : NISHIDE TAKASHI
NASHIMOTO KUNIO
ITAI TAKEO
KUMAGAI HITOSHI

(54) KEY MANAGING SERVER SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a safe and simple management method of an open key certificate and a secret key by automating a system with a key management server which manages a key management table and an application management table.
SOLUTION: When a connection request (1) to an application server 6 from a client terminal 4 is given, a key management server 1 obtains an open key certificate for application (4 and 5) from an application CA8, by using a key management table 2 (2) or an application management table 3 (3). An open key certificate for application and a secret key, which are required for certification at the time of connection with the application server 6, are transmitted to the client terminal 4 (6). The client terminal 4 is certified (7) at connection by using the open key certificate for application and the secret key, which are received from the key management server 1. If certification is successful, communication with the application server 6 can be conducted.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－49766
（P2000－49766A）
(43)公開日　平成12年２月18日(2000.2.18)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	５Ｋ０１３
9/32			６０１Ｚ	
			６７５Ｄ	

審査請求　未請求　請求項の数５　ＯＬ　（全８頁）

(21)出願番号　特願平10－210672

(22)出願日　平成10年７月27日(1998.7.27)

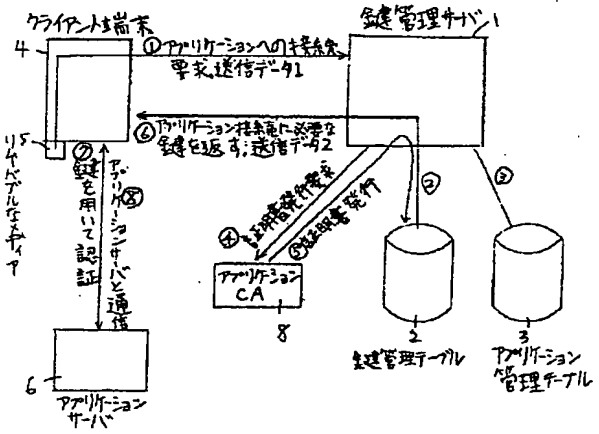
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町６丁目81番地
(72)発明者　西出　隆志
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウェアエンジニアリング株式会社内
(74)代理人　100068504
弁理士　小川　勝男

最終頁に続く

(54)【発明の名称】　鍵管理サーバシステム

(57)【要約】
【課題】ユーザが各アプリケーションに応じて公開鍵証明書と秘密鍵を使い分ける場合、ユーザにその使い分けを意識させることなく、容易な公開鍵証明書と秘密鍵の管理方法を提供すること。
【解決手段】ユーザごとの鍵管理テーブルと、各アプリケーションの情報を一括管理したアプリケーション管理テーブルを用いて、鍵の生成と、ＣＡへの公開鍵証明書発行の申請と、認証で必要な鍵のペアの取り出しを鍵管理サーバに行わさせる。

図２



1

【特許請求の範囲】

【請求項1】ユーザごとに作成した、各アプリケーションとその接続時の認証で用いられる公開鍵証明書と秘密鍵(これらをアプリケーション用の公開鍵証明書と秘密鍵と呼ぶ)のペアを管理する鍵管理テーブルと、各アプリケーションに関して接続時の認証で用いる鍵の生成アルゴリズムと認証で用いるアプリケーション用公開鍵証明書の発行を行うCA(これをアプリケーションCAと呼ぶ)と、アクセス可能なユーザ名を格納したアクセス可能ユーザリストファイルの情報を格納するアプリケーション管理テーブルを備えることを特徴とする鍵管理サーバシステム。

【請求項2】鍵管理サーバとユーザがどちらも、本鍵管理サーバシステムが信頼しているある一つのCA(これを鍵管理サーバシステムCAと呼ぶ)から発行された公開鍵証明書(これを鍵管理サーバシステム用公開鍵証明書と呼ぶ)を用いて、お互いの通信の暗号化、認証を行う通信プロトコルを有することを特徴とする鍵管理サーバシステム。

【請求項3】あるユーザが使用するクライアント端末から、あるアプリケーションサーバへの接続要求があったときに、もしそのアプリケーションサーバへの接続時の認証に必要なアプリケーション用の公開鍵証明書と秘密鍵がまだそのユーザ用の鍵管理テーブルに登録されていない場合、そのユーザがアプリケーションサーバへのアクセス権限を持つのならば、鍵管理サーバが、アプリケーション管理テーブルから鍵生成アルゴリズムを得て、自動的に公開鍵と秘密鍵のペアを生成し、アプリケーション管理テーブルからアプリケーションCAを得て、そのCAに公開鍵証明書の発行を要求し、ユーザの鍵管理テーブルに新たに、アプリケーションと生成した鍵のペアを登録することを特徴とする鍵管理サーバシステム。

【請求項4】あるユーザが使用するクライアント端末から、あるアプリケーションサーバへの接続要求があったとき、まずユーザは鍵管理サーバに接続し、鍵管理サーバが、そのユーザを鍵管理サーバシステム用公開鍵証明書とその対となる秘密鍵(これを鍵管理サーバシステム用秘密鍵と呼ぶ)を用いて認証し、認証が成功すれば、クライアント端末へアプリケーションサーバへの接続時の認証に必要なアプリケーション用の公開鍵証明書と秘密鍵をユーザの鍵管理テーブルから取り出し、公開鍵証明書の有効期限を確認し、もし有効期限が切れていたら請求項3のように公開鍵証明書をアプリケーションCAから取得し、アプリケーション用の公開鍵証明書と秘密鍵を、ユーザの鍵管理サーバシステム用公開鍵で暗号化して送ることを特徴とする鍵管理サーバシステム。

【請求項5】各ユーザは本鍵管理サーバシステムの管理者から配布された自分の鍵管理サーバシステム用の公開鍵証明書と秘密鍵と、鍵管理サーバシステムCA自身の公開鍵証明書を格納したリムーバブルメディアを所持管理し、このメディアを用いることによって鍵管理サーバから認証を受けることを特徴とする鍵管理サーバシステム。

2

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は複数の公開鍵証明書と秘密鍵を扱い、それらを各アプリーションサーバとの接続時に必要な認証ごとに使い分けるシステムにおける公開鍵証明書、秘密鍵等の管理に関する。

【0002】

【従来の技術】従来、ユーザの鍵管理に関する方法として、例えば、特開平09-223210号公報に記載の「携帯可能情報記憶媒体及びそれを用いた認証方法、認証システム」がある。

【0003】この方法は、ユーザがまずオフラインでCAに鍵の発行申請を行い、CAは発行申請を受けて申請ユーザの公開鍵と秘密鍵を生成してICカードに当該申請ユーザの公開鍵証明書と秘密鍵を書き込み、オフラインで申請ユーザにそのICカードを送付する。なお、公開鍵証明書は申請ユーザの公開鍵と当該公開鍵の真正を証明する当該CAの署名を含む。

【0004】ユーザはその受け取ったICカードの秘密鍵で署名を作成し認証に用い、そのICカードは自分で所持管理するというものである。

【0005】また一人のユーザが複数の公開鍵証明書と秘密鍵を持ち、それらを各アプリケーションサーバとの認証ごとに使い分ける場合、特別なシステムを用意しないのなら、鍵生成から公開鍵証明書発行の申請とその管理までの全てをユーザが各自で行うことが必要となる。

【0006】

【発明が解決しようとする課題】ところで上述の特開平09-223210号公報の方法では、安全にユーザが秘密鍵を管理することができるものの、1ユーザが複数の公開鍵証明書と秘密鍵を持つ場合の、その使い分けについては言及されていない。またユーザがCAに対して、公開鍵証明書の発行を要求するとき、ユーザは自らその処理を行わなければならない。さらに公開鍵、秘密鍵の生成はCAが行うという設定になっているが、そのような鍵生成を行わないCAに対して公開鍵証明書の発行を要求する場合について言及されていない。

【0007】またユーザが複数の公開鍵証明書と秘密鍵を自分で管理する方法では、アプリケーション接続時の認証に必要な公開鍵証明書と秘密鍵の使い分けや、有効期限が切れた公開鍵証明書の処理、また秘密鍵をクライアント端末の磁気ディスク等で管理する場合に、盗用を防ぐため、ユーザのパスワードで秘密鍵を暗号化するという対策をとらなければならない、等の問題がある。

【0008】本発明の目的は、ユーザにアプリケーションサーバ接続時の認証で必要となるユーザの公開鍵証明書と秘密鍵の使い分けを意識させることなく、また公開

3

鍵証明書の更新と鍵生成と公開鍵証明書発行の手続きを鍵管理サーバによって、自動化することでユーザの負担を軽減し、管理しなければならないのは鍵管理サーバシステム用の公開鍵証明書と秘密鍵の組みのみにし、これらをリムーバブルメディアに格納することによって、安全で容易な公開鍵証明書と秘密鍵の管理の方法を提供することにある。

【０００９】

【課題を解決するための手段】上記目的を達成するために、本発明では、ユーザごとに作成した各アプリケーションとその接続時の認証で用いられるアプリケーション用の公開鍵証明書と秘密鍵のペアを管理する鍵管理テーブルと、各アプリケーションに関して接続時の認証で用いる鍵の生成アルゴリズムと、認証で用いるアプリケーション用公開鍵証明書の発行を行うアプリケーションＣＡと、アクセス可能なユーザ名を格納したアクセス可能ユーザリストファイルの情報を格納するアプリケーション管理テーブルと、これら鍵管理テーブルとアプリケーション管理テーブルを管理し、ユーザからのアプリケーション接続要求が来たときに、ユーザがアプリケーションサーバへのアクセス権限を持ち、認証に必要なアプリケーション用の公開鍵証明書と秘密鍵がそのユーザの鍵管理テーブルに存在しなければ、または存在しても公開鍵証明書の有効期限が切れていれば、アプリケーションＣＡに対して、そのＣＡが鍵生成を行わないなら鍵生成を行ってから、ユーザの代わりに公開鍵証明書発行の申請を出し、アプリケーション用秘密鍵とアプリケーションＣＡから受け取ったアプリケーション用公開鍵証明書をユーザの鍵管理テーブルに登録し、これらの公開鍵証明書と秘密鍵をユーザの使用するクライアント端末へ送信する鍵管理サーバなるものを備えることを特徴とする。

【００１０】さらに、本発明では鍵管理サーバとユーザは本鍵管理サーバシステムが信頼する鍵管理サーバシステムＣＡから発行された鍵管理サーバシステム用の公開鍵証明書と秘密鍵を用いてお互いを認証し、ユーザは本鍵管理サーバシステムの管理者から配布された、ユーザの鍵管理サーバシステム用の公開鍵証明書と秘密鍵と、鍵管理サーバシステムＣＡ自身の公開鍵証明書を格納するリムーバブルメディアを所持管理し、アプリケーションサーバと接続が必要なときだけそのリムーバブルメディアをメディアのリーダにセットし、鍵管理サーバから認証を受け、アプリケーションサーバへの接続に必要なアプリケーション用の公開鍵証明書と秘密鍵を受信することを特徴とする。

【００１１】

【発明の実施の形態】以下、本発明を実施する場合の一形態を図面を参照して具体的に説明する。

【００１２】図1は、本発明実施の一形態の鍵管理サーバシステムの構成を示すブロック図である。

4

【００１３】１は、ユーザの鍵管理等を行う鍵管理サーバであり、鍵管理テーブル2とアプリケーション管理テーブル3と複数のクライアント端末4を管理する。

【００１４】２は、鍵管理サーバ1が管理するユーザごとにアプリケーションとそのアプリケーション接続時の認証に用いるアプリケーション用の公開鍵証明書と秘密鍵の対応情報を格納している鍵管理テーブルであり、詳細を図3に示している。

【００１５】３は、各アプリケーションとの接続時の認証で用いる鍵の生成アルゴリズムと、当該アプリケーション用公開鍵証明書の発行を行うアプリケーションＣＡ８と、当該アプリケーションにアクセス可能なユーザ名を格納したアクセス可能ユーザリストファイルの情報を格納するアプリケーション管理テーブルであり、詳細を図4に示している。

【００１６】４はクライアント端末、５はクライアント端末4から読み込み可能なリムーバブルメディア、６は各種アプリケーションサーバである。

【００１７】７は、本鍵管理サーバシステムが信頼し、本鍵管理サーバシステムに登録されたユーザと鍵管理サーバ1間の通信の暗号化に用いる鍵管理サーバシステム用公開鍵証明書を発行する鍵管理サーバシステムＣＡである。

【００１８】８は、各アプリケーションサーバ6が接続時の認証で用いるアプリケーション用公開鍵証明書の発行を行うアプリケーションごとのアプリケーションＣＡであり、各アプリケーションサーバ6が指定したＣＡである。

【００１９】図2は本鍵管理サーバシステムでの、クライアント端末4と、鍵管理サーバ1と、アプリケーションサーバ6と、アプリケーションサーバ6が認証で用いるアプリケーション用公開鍵証明書の発行をするアプリケーションＣＡ８の間のデータのやりとりの概略を示すブロック図である。図2に基づいて、鍵管理サーバシステムの概略動作を次に説明する。

【００２０】ユーザがアプリケーションサーバ6との接続を要求するとき、クライアント端末4はまず鍵管理サーバ1と接続し、アプリケーションサーバ6との接続時の認証に必要なアプリケーション用の公開鍵証明書と秘密鍵を鍵管理サーバ1から取得し、それらを用いてアプリケーションサーバ6に接続して認証を受け、通信を行う。

【００２１】アプリケーションサーバ6はクライアント端末4から接続要求があると、クライアント端末4を使用しているユーザのアプリケーション用の公開鍵証明書と秘密鍵を用いて、ユーザを認証し、認証すれば、クライアント端末4と通信を開始する。

【００２２】これをもう少し具体化して説明する。

【００２３】鍵管理サーバ1はクライアント端末4からのアプリケーションサーバ6への接続要求(①)がある

5

と、鍵管理テーブル2 (②)を用いて、またはアプリケーション管理テーブル3 (③)を用いて、アプリケーションＣＡ８よりアプリケーション用公開鍵証明書を取得する (④, ⑤)。そして、クライアント端末4 にアプリケーションサーバ6 との接続時の認証に必要なアプリケーション用の公開鍵証明書と秘密鍵をクライアント端末4 に送信する (⑥)。クライアント端末4 は鍵管理サーバ1 より受け取ったアプリケーション用の公開鍵証明書と秘密鍵を用いて、アプリケーションサーバ6 との接続時に認証を受け (⑦)、認証に成功すればアプリケーションサーバと通信することができる (⑧)。

【００２４】鍵管理サーバ1 のさらに詳細な動作を次に説明する。

【００２５】鍵管理サーバ1 は、ユーザの使用するクライアント端末4 からアプリケーションサーバ6 への接続要求を受けて、当該アプリケーション接続時の認証に必要なアプリケーション用の公開鍵証明書と秘密鍵が鍵管理テーブル2 に存在するかどうか調べる。存在するならば鍵管理テーブル2 から取り出し、それらをクライアント端末4 へ送信する。存在しなければ、アプリケーション管理テーブル3 からアプリケーション用公開鍵証明書発行要求を送るアプリケーションＣＡ８を得て、もしアプリケーションＣＡ８が鍵生成を行わないなら鍵生成アルゴリズムから鍵を生成し、アプリケーションＣＡ８へアプリケーション用公開鍵証明書発行の要求を送り、アプリケーション用秘密鍵とアプリケーションＣＡ８から受け取ったアプリケーション用公開鍵証明書をユーザの鍵管理テーブル2 へ登録し、この秘密鍵と公開鍵証明書をクライアント端末4 へ送信する。

【００２６】なお、この鍵管理サーバ1 とクライアント端末4 の間の通信は、鍵管理サーバシステムＣＡ７から鍵管理サーバ1 とユーザに対して発行される鍵管理サーバシステム用公開鍵証明書とその対となる鍵管理サーバシステム用秘密鍵を用いて暗号化されている。

【００２７】次に鍵管理テーブル2 の構成を図3 に示す。ユーザ一人につき一つこのテーブルが作成され、ユーザが接続を要求するアプリケーションサーバ6 に応じて、その接続時の認証に必要となるアプリケーション用の公開鍵証明書と秘密鍵が取り出されるようになっている。また鍵管理テーブル2 は鍵管理サーバ1 の鍵管理サーバシステム用公開鍵で暗号化されている。

【００２８】次にアプリケーション管理テーブル3 の構成を図4 に示す。各アプリケーションサーバ6 につき接続時の認証で必要なアプリケーション用公開鍵証明書を発行するアプリケーションＣＡ８と、アプリケーションＣＡ８が鍵生成を行わない場合に必要となる鍵生成アルゴリズムとアクセス可能なユーザ名を格納したアクセス可能ユーザリストファイルからなる。

【００２９】ユーザは本鍵管理サーバシステムの管理者から配布される、鍵管理サーバシステムＣＡ７から発行

6

された鍵管理サーバシステム用公開鍵証明書とその対となる鍵管理サーバシステム用秘密鍵と、鍵管理サーバシステムＣＡ７自身の公開鍵証明書が格納されたリムーバブルメディア5 さえあれば、アプリケーション用公開鍵証明書の取得、鍵生成、アプリケーションごとの鍵の使い分けを意識せずに行うことができる。

【００３０】図5 はユーザが本鍵管理サーバシステムの管理者から配布されて、所持管理するリムーバブルメディア5 に格納された内容を示す。これはユーザの鍵管理サーバシステム用の公開鍵証明書と秘密鍵と、鍵管理サーバシステムＣＡ７自身の公開鍵証明書からなる。ユーザは本鍵管理サーバシステムに登録され、このリムーバブルメディア5 に格納された情報を持つだけで、鍵管理サーバ1 から認証を受けることが出来、自分がアクセス権限を持っているアプリケーションサーバ6 と接続時の認証におけるアプリケーション用の公開鍵証明書と秘密鍵の使い分けを意識することなく通信できる。

【００３１】図6 はクライアント端末4 のアプリケーションサーバ6 への接続要求を行うときの処理手順を示すフローチャートである。図6 において、まずユーザから鍵管理サーバ1 へアプリケーションサーバ6 への接続要求が出され(ステップ６０１)、クライアント端末4 はリムーバブルメディア5 からユーザの鍵管理サーバシステム用の公開鍵証明書と秘密鍵と、鍵管理サーバシステムＣＡ７自身の公開鍵証明書を取り出し(ステップ６０２)、鍵管理サーバ1 への送信データ１を作成(ステップ６０３)し、この送信データ１へユーザの鍵管理サーバシステム用秘密鍵で署名をする(ステップ６０４)。この送信データ１は図8 に示される内容になる。

【００３２】次に鍵管理サーバ1 へ作成した送信データ１を送信し(ステップ６０５)、そして鍵管理サーバ1 から送信されてきた送信データ２を受信する(ステップ６０６)。クライアント端末は鍵管理サーバ1 から送信されてきた送信データ２をユーザの鍵管理サーバシステム用秘密鍵で復号する(ステップ６０７)。次に受信した送信データ２に含まれる鍵管理サーバ1 の鍵管理サーバシステム用公開鍵証明書の署名の確認を鍵管理サーバシステムＣＡ７自身の公開鍵を用いて行い(ステップ６０８)、鍵管理サーバ1 から送信されてきた送信データ２の図9 の項番1 ～4 に対する署名(図9 の項番5)の確認を鍵管理サーバ1 の公開鍵を用いて行い(ステップ６０９)、アプリケーションサーバ6 との接続時の認証に必要なアプリケーション用の公開鍵証明書と秘密鍵を取得する(ステップ６１０)。クライアント端末4 はこうして受信したアプリケーション用の公開鍵証明書と秘密鍵を用いてアプリケーションサーバ6 ごとのプロトコルに従った認証を受ける(ステップ６１１)。

【００３３】図7 は鍵管理サーバ1 のクライアント端末4 からアプリケーションサーバ6 への接続要求が発生したときの処理手順を示すフローチャートである。図7 に

7

おいて、まずクライアント端末4から送信されるアプリケーションサーバ6への接続要求の送信データ１を受信し（ステップ７０１）、鍵管理サーバ1がキャッシュしているまたは必要ならば鍵管理サーバシステムＣＡ７より取得した鍵管理サーバシステムＣＡ７自身の公開鍵証明書で送信データ１の中のユーザの鍵管理サーバシステム用公開鍵証明書（図8の項番２）の署名を確認する（ステップ７０２）。

【００３４】次にクライアント端末4から受信した送信データ１の署名（図8の項番3）をユーザの鍵管理サーバシステム用公開鍵（図8の項番２）を用いて確認し（ステップ７０３）、ユーザがアプリケーションサーバ6との接続時の認証で必要なアプリケーション用の公開鍵証明書と秘密鍵を鍵管理テーブル2から検索する（ステップ７０４）。アクセス可能ユーザリストファイルにそのユーザ名があるかどうかで判定するアプリケーションサーバ6へのアクセス権限と、鍵の有無と、もし鍵が存在すればそのアプリケーション用公開鍵証明書の有効期限の検査をし（ステップ７０５）、鍵のペアが無いまたは有効期限が切れているなら、アプリケーション管理テーブル3を用い、アプリケーションＣＡ８が鍵生成を行わないなら鍵生成を行い（ステップ７０６）、アプリケーションＣＡ８からアプリケーション用公開鍵証明書を取得する（ステップ７０７）。

【００３５】もしユーザがそのアプリケーションサーバ6に対してアクセス権限を持たないなら、クライアント端末4にエラーシグナルを送信し（ステップ７１１）、クライアント端末4はこのシグナルを受けてエラーで終了する。次にクライアント端末4への送信データ２を作成し（ステップ７０８）、送信データ２に鍵管理サーバ１の鍵管理サーバシステム用秘密鍵で署名する（ステップ７０９）。この送信データ２は図9に示される内容になる。そしてクライアント端末4より受信した送信データ１の中のユーザの鍵管理サーバシステム用公開鍵（図８の項番2）でこの送信データ２を暗号化してクライアント端末4へ送信する（ステップ７１０）。

【００３６】この鍵管理サーバシステムを運用するにあたって、まず鍵管理サーバシステムＣＡ７を既存のＣＡから選定またはこのシステム用に開設する。そして各アプリケーションサーバ6に関して接続時の認証で用いる鍵の生成アルゴリズムと、認証で用いるアプリケーション用公開鍵証明書の発行を行うアプリケーションＣＡ８と、アクセス可能なユーザ名を格納したアクセス可能ユーザリストファイルの情報を格納するアプリケーション管理テーブル3を作成する。

【００３７】そして、ユーザは鍵管理サーバ1への登録を本鍵管理サーバシステムの管理者に依頼する。この登録によって鍵管理サーバ1にユーザの鍵管理テーブル2が作成される。そしてユーザがどのアプリケーションを利用出来るか決定し、アプリケーション管理テーブルから参照されるアクセス可能なユーザ名を格納したアクセス可能ユーザリストファイルを変更する。

8

【００３８】そして本鍵管理サーバシステムの管理者は、ユーザがこの鍵管理サーバシステムで用いる鍵管理サーバシステム用の公開鍵と秘密鍵を生成し、鍵管理サーバシステムＣＡ７から鍵管理サーバシステム用公開鍵証明書を発行してもらい、これらの鍵管理サーバシステム用の公開鍵証明書と秘密鍵と、鍵管理サーバシステムＣＡ７の公開鍵証明書をリムーバブルメディア5に格納し、ユーザに配布する。ユーザは鍵管理サーバ1を介してアプリケーションサーバ6と接続するときだけ、リムーバブルメディア5をメディアのリーダにセットしアプリケーションサーバとの接続時の認証に必要となるアプリケーション用の公開鍵証明書と秘密鍵を受信する。

【００３９】ここで、鍵管理サーバ1が管理するユーザのアプリケーション用の公開鍵証明書と秘密鍵は、鍵管理サーバ1の鍵管理サーバシステム用公開鍵で暗号化してあるが、第三者による不正なアクセスがなされることのない環境に置かれることが望ましい。

【００４０】

【発明の効果】以上、説明したように本発明によれば、ユーザは一組みの鍵管理サーバシステム用の公開鍵証明書と秘密鍵を安全なリムーバブルメディアで管理するだけでよくなる。そして複数のアプリケーションサーバごとの接続時の認証で必要となるアプリケーション用の公開鍵証明書と秘密鍵の使い分けを意識する必要がなくなり、煩雑な鍵管理から解放される。また、鍵管理サーバが鍵生成とアプリケーション用公開鍵証明書の取得を自動的に行ってくれるのでユーザの負担が軽減される。さらに各アプリケーションの情報は、鍵管理サーバが管理するアプリケーション管理テーブルで一括して管理されるので、変更があっても容易に対応することができる。

【図面の簡単な説明】

【図1】本発明である鍵管理サーバシステムの実施の一形態の概略構成を示すブロック図。

【図2】本鍵管理サーバシステムにおけるクライアント端末と、鍵管理サーバと、アプリケーションサーバとアプリケーションＣＡ間のデータのやりとりの概略を示すブロック図。

【図3】鍵管理サーバが管理するユーザごとのアプリケーションとアプリケーション用の公開鍵証明書と秘密鍵の対応を表す鍵管理テーブル。

【図4】アプリケーションＣＡと鍵生成が必要な場合の鍵生成アルゴリズムとアクセス可能なユーザ名を格納したアクセス可能ユーザリストファイルを表すアプリケーション管理テーブルを示す図。

【図5】各ユーザが所持管理するリムーバブルメディアに格納される内容を表す図。

【図6】クライアント端末のアプリケーションサーバへの接続要求を行うときの処理手順の概要を示すフローチ

ャート。

【図7】鍵管理サーバのクライアント端末からアプリケーションサーバへの接続要求が発生したときの処理手順の概要を示すフローチャート。

【図8】クライアント端末と鍵管理サーバ間のデータのやりとりで、クライアント端末から鍵管理サーバへ送信される送信データ1の形式を示す図。

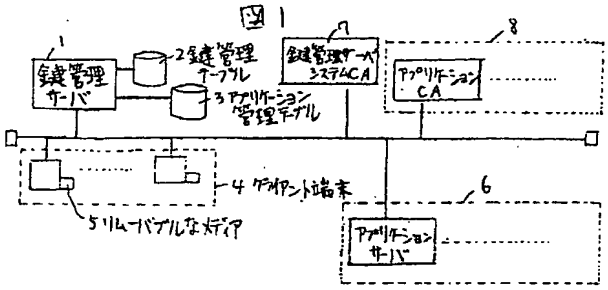
【図9】クライアント端末と鍵管理サーバ間のデータのやりとりで、鍵管理サーバからクライアント端末へ送信される送信データ2の形式を示す図。

【符号の説明】

1…鍵管理サーバ、2…鍵管理テーブル、3…アプリケーション管理テーブル、4…クライアント端末、5…リムーバブルメディア、6…アプリケーションサーバ、7…鍵管理サーバシステムCA、8…各アプリケーションサーバが接続時の認証で用いるアプリケーション用公開鍵証明書の発行を行うアプリケーションCA。

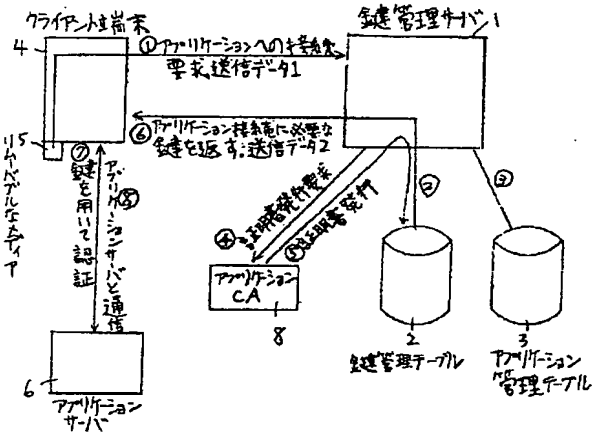
【図1】

図1



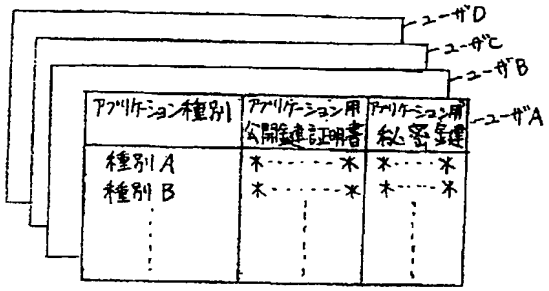
【図2】

図2



【図3】

図3



【図4】

図4

アプリケーション種別	証明書発行するCA	鍵生成アルゴリズム	アクセス可能ユーザリストファイル
種別A	CA8A	—	AuserFile
種別B	CA8B	*	BuserFile
⋮	⋮	⋮	⋮

【図5】

図5

鍵管理サーバシステム用公開鍵証明書
鍵管理サーバシステム用秘密鍵
鍵管理サーバシステムCAの公開鍵証明書

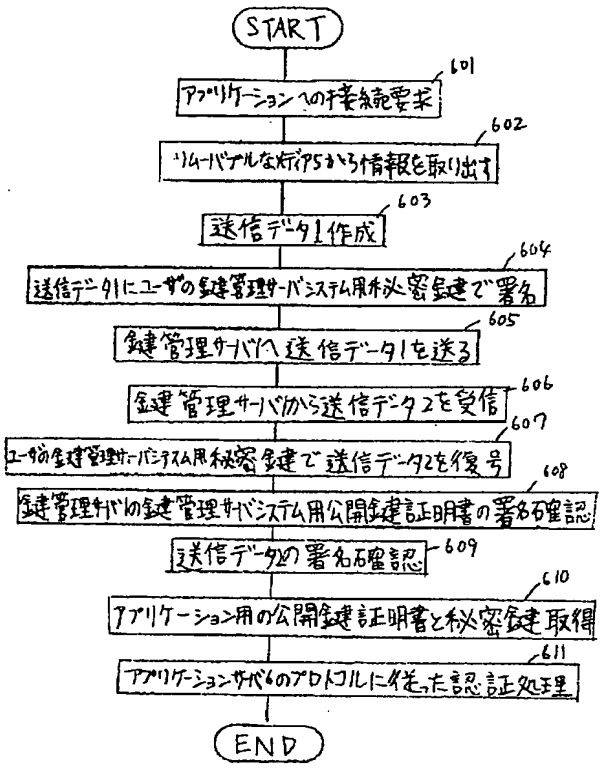
【図8】

図8

1	アプリケーション種別
2	ユーザの鍵管理サーバシステム用公開鍵証明書
3	1,2に対するユーザの鍵管理サーバシステム用秘密鍵による署名

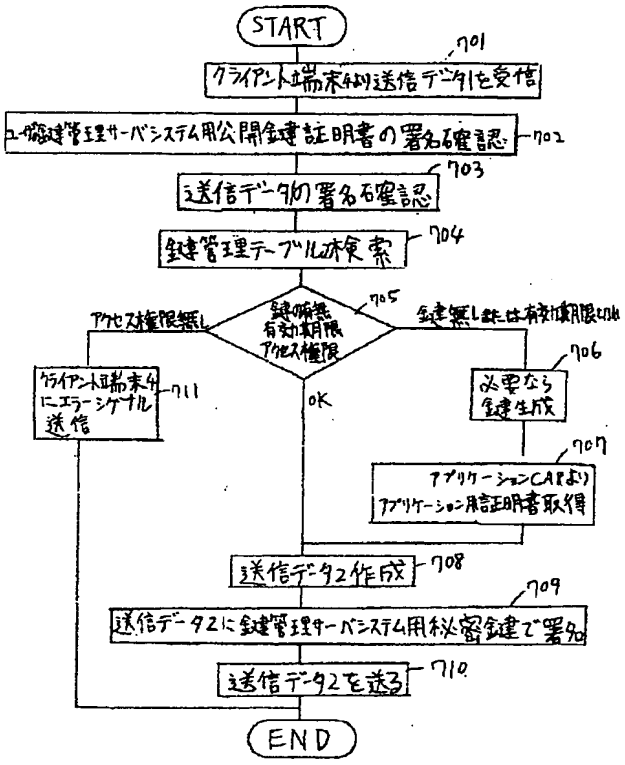
【 図6 】

図6



【 図7 】

図7



【 図9 】

図9

1	アプリケーション種別
2	アプリケーション接続時の認証に必要なユーザのアプリケーション用公開鍵証明書
3	アプリケーション接続時の認証に必要なユーザのアプリケーション用秘密鍵
4	鍵管理サバの鍵管理サバシステム用公開鍵証明書
5	1～4に対する鍵管理サバの鍵管理サバシステム用秘密鍵による署名

フロント ページの続き

(72)発明者　梨本　邦夫
神奈川県横浜市中区尾上町6 丁目81番地
日立ソフトウェアエンジニアリング株式会社内

(72)発明者　板井　健雄
神奈川県横浜市中区尾上町6 丁目81番地
日立ソフトウェアエンジニアリング株式会社内

(72)発明者　熊谷　仁志
神奈川県横浜市中区尾上町6 丁目81番地
日立ソフトウェアエンジニアリング株式会
社内

Fターム(参考)　5K013 BA02 EA06 GA08